Claims

[c1] 1.A secure external mass storage device comprising:

a host interface, for coupling the secure external mass storage device to a host computer, the host computer reading data from the secure external mass storage device through the host interface;

a memory media with a protected memory area, for storing data for access by an authorized user of the host computer;

a biometric reader that generates biometric data from the authorized user; and

a controller that executes an initialization routine, the controller coupled to the biometric reader to accept the biometric data from the biometric reader, the controller comparing the biometric data to a biometric record to determine when the biometric data is for the authorized user, the controller blocking access to the protected memory area when the biometric data is not for the authorized user,

whereby the host computer is blocked from accessing the protected memory area when the biometric reader does not input the biometric data for the authorized user.

[c2] 2.The secure external mass storage device of claim 1 wherein the biometric record is stored on the memory media or on a firmware memory accessible by the controller;

wherein the initialization routine is stored on the memory media or on a firmware memory accessible by the controller.

[c3] 3.The secure external mass storage device of claim 2 wherein the biometric record is not stored on the host computer,

wherein when the secure external mass storage device is connected to a different host computer, the initialization routine is executed to compare new biometric data from the biometric reader to the biometric record before authorizing access of the protected memory area,

whereby the secure external mass storage device does not rely on the host computer for security but is secure when connected to other host computers.

[c4] 4.The secure external mass storage device of claim 2 wherein the controller is part of a microcontroller that includes the firmware memory.

[c5] 5.The secure external mass storage device of claim 4 further comprising:
a biometric interrupt, generated by the biometric reader when biometric data is available, for signaling the controller to read the biometric data.

[c6] 6.The secure external mass storage device of claim 2 wherein the memory media also comprises an unprotected memory area;
wherein the controller allows access of the unprotected memory area but not the protected memory area when the biometric data is not for the authorized user.

[c7] 7.The secure external mass storage device of claim 2 wherein the biometric reader is a fingerprint reader, a hand-print reader, a facial geometry scanner, an iris reader, a retina scanner, or a voice-print recognizer.

[c8] 8.The secure external mass storage device of claim 2 wherein the host interface is for connection to a port on the host computer that uses a universal-serial bus (USB), IEEE 1394, Personal-Computer Memory Card International Association (PCMCIA), parallel port, or small-computer-system-interface (SCSI) protocol.

[c9] 9.The secure external mass storage device of claim 2 wherein the memory media is a magnetic disk, an optical disk, or a solid-state memory.

[c10] 10.The secure external mass storage device of claim 9 wherein the memory media is removable from the secure external mass storage device,
wherein the initialization routine is activated when the memory media is inserted into the secure external mass storage device or when the host interface is connected to the host computer.

[c11] 11.A method for securing an external mass storage comprising:
activating an initialization routine when an external mass storage device is connected to a host;

executing the initialization routine stored in the external mass storage device by reading a firmware memory containing the initialization routine;
activating a biometric input to capture biometric information from a user;
comparing the biometric information to a biometric record for an authorized user to determine when the biometric information matches within a threshold;
when the biometric information matches, continuing to execute the initialization routine to mount the external mass storage to the host, allowing the host to access protected data in the external mass storage; and
when the biometric information does not match, halting execution of the initialization routine to prevent mounting of the external mass storage to the host, preventing the host from accessing protected data in the external mass storage,
whereby the initialization routine authenticates biometric information when the external mass storage is connected to the host.

[c12] 12.The method of claim 11 further comprising:
reading the biometric record from non-volatile memory in the external mass storage device,
whereby the biometric record for the authorized user is stored on the external mass storage device.

[c13] 13.The method of claim 11 wherein the external mass storage accepts a removable media containing the protected data;
wherein the initialization routine is activated when the removable media is plugged into the external mass storage device.

[c14] 14.The method of claim 11 further comprising:
activating a biometric interrupt to signal the initialization routine when the biometric input captures the biometric information.

[c15] 15.The method of claim 11 wherein several authorized users have biometric records stored on the external mass storage device;
further comprising:

comparing the biometric information to a plurality of biometric records to find a closest match, and allowing access to the protected data when the closest match is within the threshold.

[c16] 16.The method of claim 11 further comprising:
when a first use of the external mass storage occurs, executing an installation routine, the installation routine:
activating the biometric input to capture biometric information from a new user;
forming a biometric template from the biometric information;
re-activating the biometric input to capture additional biometric information from the new user;
comparing the additional biometric information to the biometric template for the new user to determine when the additional biometric information matches within a threshold;
when the biometric information matches, storing the biometric template as the biometric record for the new user, the new user being the authorized user; and
when the biometric information does not match, re-activating the biometric input to re-capture the biometric information from the new user and replacing the biometric template with a new biometric template, re-activating the biometric input and capturing and comparing the additional biometric information to verify the new biometric template,
whereby the biometric template for the new user is stored upon installation.

[c17] 17.An external peripheral comprising:
host interface means for coupling the external peripheral to a host computer;
controller means, coupled to the host interface means, for executing programmable routines;
memory means, coupled to the controller means, for storing data from the host computer, the memory means having protected memory means for storing data for access by an authorized user of the host computer; and

biometric reader means, coupled to the controller means, for generating biometric data from the authorized user;

the controller means for accepting the biometric data from the biometric reader means, comparing the biometric data to a biometric record to determine when the biometric data is for the authorized user, and for blocking access to the protected memory means when the biometric data is not for the authorized user,

whereby the host computer is blocked from accessing protected memory when the biometric data is not for the authorized user.

[c18] 18.The external peripheral of claim 17 wherein the controller means including an execution means for executing instructions, a code memory means for storing the programmable routines, and a storage controller means for accessing the memory means.

[c19] 19.The external peripheral of claim 18 wherein the biometric record is stored in the code memory means.

[c20] 20.The external peripheral of claim 17 wherein the biometric record comprises data for locations where finger lines or patterns change direction or end.